

U. S. Department of Agriculture
Washington, D.C. 20250

DEPARTMENTAL ADMINISTRATION INSTRUCTION		DA-200-1	
SUBJECT: Information Technology Security Policy		ORIGINATING OFFICE:	Office of Operations
REPLACES: N/A		DISTRIBUTION:	All Departmental Administration Offices
APPLIES TO: All Departmental Administration Offices		EXPIRES:	When superseded or cancelled.
APPROVED BY: /s/ <i>John Surina</i> John Surina Deputy Assistant Secretary for Administration		EFFECTIVE DATE: May 18, 2004	

TABLE OF CONTENTS

<u>Chapter</u>	<u>Page</u>
CHAPTER 1: INTRODUCTION.....	1
1 PURPOSE.....	1
2 INTRODUCTION	1
3 SCOPE.....	1
4 POLICY.....	2
5 ROLES AND RESPONSIBILITIES	2
6 DA IT SYSTEM OPERATIONS	3
7 RECORDS AND REPORTS.....	4
8 AUTHORITIES AND REFERENCES	4
9 GLOSSARY	4
CHAPTER 2: MANAGEMENT CONTROLS.....	5
1 INFORMATION SENSITIVITY	5
2 RISK MANAGEMENT	6
3 SECURITY CONTROLS REVIEW	6

4	RULES OF BEHAVIOR.....	8
5	LIFE CYCLE SECURITY MANAGEMENT.....	9
6	CONFIGURATION CHANGE MANAGEMENT	10
7	CERTIFICATION AND ACCREDITATION	11
8	SYSTEM SECURITY PLAN.....	12
CHAPTER 3: OPERATIONAL CONTROLS		13
1	PERSONNEL SECURITY.....	13
2	PHYSICAL AND ENVIRONMENTAL SECURITY	14
3	PRODUCTION, INPUT/OUTPUT CONTROLS	16
4	CONTINGENCY AND DISASTER RECOVERY PLANNING	17
5	HARDWARE AND SOFTWARE SYSTEM MAINTENANCE	17
6	DATA INTEGRITY	19
7	DOCUMENTATION	19
8	SECURITY AWARENESS AND TRAINING.....	20
9	INCIDENT HANDLING, RESPONSE, AND REPORTING.....	21
CHAPTER 4: TECHNICAL CONTROLS.....		23
1	IDENTIFICATION AND AUTHENTICATION.....	23
2	LOGICAL ACCESS CONTROL.....	24
3	AUDIT TRAILS.....	25
APPENDIX A: AUTHORITIES AND REFERENCES.....		A-1
APPENDIX B: TERMS AND DEFINITIONS		B-1
APPENDIX C: ACRONYMS AND ABBREVIATIONS.....		C-1
APPENDIX D: DA POLICY ON USE OF PERSONAL ELECTRONIC DEVICES		D-1

CHAPTER 1 INTRODUCTION

1 PURPOSE

This Information Technology (IT) Security Policy Instruction establishes the policy, responsibilities, and security requirements of the Information Technology Security Program (ITSP) for the Departmental Administration (DA). These policies are required by and consistent with:

- a Pertinent legislation including the Federal Information Security Management Act (FISMA);
- b Government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration, and the Office of Personnel Management; and
- c Department of Agriculture policies, standards, and procedures such as Applications System Life Cycle Management and Software Management.

The full list of authorities and references used to determine the security requirements embodied in this document are listed in Appendix A.

2 INTRODUCTION

DA is the central organization within USDA responsible for the leadership and oversight of administrative management activities in each USDA mission area and Departmental Staff Office. It maintains automated information systems that require controls to assure security of data contained within the systems.

This Instruction addresses the management, operational, and technical controls that form the basis for an effective IT security program. It provides direction for protecting the availability, integrity, confidentiality, and continuity of information contained in DA IT systems. Detailed information relating to the implementation of these policies is provided in the DA Information Technology Security Procedural Guidance.

3 SCOPE

The policies contained in this Instruction apply to all DA Offices and to all applications and systems categorized as a major application (MA) or a general support system (GSS). It covers all agency information collected, processed, transmitted, stored, or disseminated through the use of an MA or GSS or wireless device. Definitions for a major application and a general support system can be found in Appendix B, Terms and Definitions. All non-major applications developed within the GSS are covered under the scope of the GSS security purview.

4 POLICY

This Instruction describes the basic IT security policy by defining the management controls, operational controls, and production, input/output controls required for effective IT security. The IT security controls set forth in this section apply to all DA personnel, including contractors, who design, implement, manage, and maintain DA IT systems. The manner in which they interact with the GSS, MA, and each other when using local and DA-wide IT systems is an important aspect of personnel security. The sensitive nature of the information in DA IT systems mandates that the requirements below and USDA personnel policies be applied to DA IT systems personnel.

DA IT systems must be protected from damage or destruction by manmade and non-manmade occurrences. Additionally, DA IT support activities require that controls be established to ensure the adequate security of input, production, and output support processes. DA will develop and maintain an IT Contingency/Disaster Recovery Plan.

To reduce threats to the integrity, confidentiality, and availability of the information in DA IT systems, strong controls related to hardware and software installation, maintenance and upgrading must be implemented. All DA IT systems require management approval to operate from the CIO.

These policies apply to any outside organizations, including contractor organizations, or their representatives, who are granted access to DA's IT resources. The general public, accessing publicly available DA Web sites, is excluded from this definition.

5 ROLES AND RESPONSIBILITIES

The basic roles and responsibilities described below may be delegated unless otherwise noted. Additional information related to the assignment of duties to fulfill the requirements of the DA IT Security Program is found in DR 3140-001, "USDA Information Systems Security Policy" and the DA Cyber Security Program Plan. More specific responsibilities are described throughout this instruction, categorized by subject area.

- a The Assistant Secretary for Administration has the overall responsibility to ensure that DA information systems are protected commensurate with the risk to the systems and the information they contain. DA security policies, procedures, and practices will be in accordance with all relevant federal laws, regulations, and guidelines, and with pertinent USDA policies.
- b The Designated Approving Authority (DAA) is responsible for the security of information within his/her organization. The DAA must ensure the protection and continuity of organizational computer systems, networks, and data operations. The DAA has the authority to decide on accepting the security safeguards and

risks for an automated information system. The Assistant Secretary for Administration or designee will be delegated this authority.

- c The Director, Office of Operations (OO) has responsibility for the security of DA computer networks and telecommunications infrastructures.
- d The DA Information Resources Director, in the role of DA Chief Information Officer (CIO), is responsible for developing and promulgating DA IT security policy and procedures. The DA CIO appoints a DA Information Systems Security Program Manager within the CIO office. The DA CIO ensures that DA staff offices appoint an Information Systems Security Program Manager (ISSPM), if needed. The detailed responsibilities and duties of these appointees can be found in this document and its associated procedures.
- e The DA IT System Security Program Manager (ISSPM) manages the DA security program and ensures DA security policies, procedures, and practices are in accordance with all relevant USDA policies and procedures and federal laws, regulations, and guidelines. The DA ISSPM provides information systems security support to DA staff offices that do not have their own ISSPM.
- f Each Staff Office Director within DA is responsible for assuring that the systems under their control or used by their office conform to the security policy and procedures established by the Assistant Secretary for Administration.
- h The ISSPM for each program office is responsible for coordinating, defining, and implementing security policies and procedures for all GSS and MA systems in their offices.
- i IT professionals and end users of DA systems are responsible for adhering to all DA information security policies, system security requirements as contained in their system security plans, and rules of behavior regarding system operation.

6 DA IT SYSTEM OPERATIONS

All DA IT systems require management approval to operate from the CIO. This approval is obtained through the certification and accreditation (C&A) process specified within this document. This policy instruction applies to the full life cycle of all systems development, hardware, software, firmware media, and facilities used to support the DA mission. The life cycle includes, but is not limited to, all actions related to a system from its inception or procurement to its replacement, removal, and/or destruction. It also applies to any changes to DA IT systems.

7 RECORDS AND REPORTS

All records and reports established by this guide and all other DA IT security-related documents will be developed and managed in accordance with current USDA and DA record and report requirements.

8 AUTHORITIES AND REFERENCES

All authorities and references used to determine the requirements for this document are listed in Appendix A.

9 GLOSSARY

Appendix B provides the terms and definitions used in this document. Appendix C contains acronyms and abbreviations used in this document.

CHAPTER 2 MANAGEMENT CONTROLS

1 INFORMATION SENSITIVITY

The following security management controls describe the basic DA IT security policy. Procedural requirements and more detailed information for each program element are found in the documents listed in Appendix A, Authorities and References. A determination of information sensitivity is the basis for security planning for each GSS and MA.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that the information sensitivity of all DA GSSs and MAs has been addressed according to the guidelines established.

Staff Office Directors are responsible for ensuring that information sensitivity has been determined for each GSS and MA under their control and that appropriate steps are taken to protect the integrity and use of the information once this determination is made.

b REQUIREMENTS

Information sensitivity within each GSS or MA must be determined in order to develop and maintain the appropriate security procedures. The information sensitivity determination must address the following elements as appropriate: confidentiality, integrity, and availability.

Confidentiality denotes the extent to which the information contained in the system requires protection from disclosure.

Integrity refers to the extent to which the information contained in the system must be protected from unauthorized, unanticipated, or unintentional modification.

Availability refers to the need for the information or services to be available on a timely basis to meet mission requirements or to avoid substantial losses.

Within these elements, the information contained in the systems should be categorized as having high, medium or low protection requirements.

Any laws, regulations, or policies that establish specific requirements should be referenced in the discussion of sensitivity. The sensitivity analysis should be summarized in a general protection statement for the system.

2 RISK MANAGEMENT

Risk management covers assessing the acceptable level of risk for a GSS or MA and determining appropriate safeguards. Risk management procedures must be established for DA systems throughout their life cycles, including any changes or modifications to them. Risk assessments must also include the use, or potential use, of Personal Electronic Devices (PED's) to access, upload, or download information from the DA GSS or its MAs.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that risk and vulnerability assessments of DA GSSs and MAs are conducted as required by the appropriate federal authorities. The DA CIO ensures all threats, as described in this document, that would prevent effective operation of DA IT systems, are communicated per the Incident Reporting Procedures and that appropriate actions are taken promptly to protect DA computer assets.

Staff Office Directors are responsible for implementing risk management procedures and for ensuring that risk and vulnerability assessments are carried out for each GSS and MA under their control.

b REQUIREMENTS

Risk assessments must be performed throughout the life cycles of every GSS and MA, using guidance established by USDA's Cyber Security Office. Information Systems Security Assessment Guide. Risk assessments must be performed, at a minimum, every three years; as a result of an adverse finding from a security controls review; or whenever significant changes are made to a system, its architecture, or any of its major applications.

Risk assessments must consider criticality and the results of vulnerability assessments in determining that the level of acceptable risk for a system is commensurate with the requirements of the system for confidentiality, integrity, and availability. Vulnerability assessments consider weaknesses relating to the platform, personnel, physical environment, and communications aspects of the MA or GSS, including access by PED's. Known security problems, configuration errors, and the installation of hardware/software "patches" are also considered.

The results of the risk assessment will be a major guide in DA's determination on whether to allow the use of PED's in its GSS or MAs.

3 SECURITY CONTROLS REVIEW

OMB Circular A-130 directs that a review of security controls be conducted periodically, but at least every three (3) years, on GSS and MA systems to assure that these controls continue to be effective. To appropriately manage risks and ensure the security of DA IT

systems, a review of the controls of all systems that are interconnected with DA IT systems must be conducted.

Reviews that result in the reporting of weaknesses or deficiencies must be accompanied by a corrective action plan for remedying those weaknesses or deficiencies.

a **ROLES AND RESPONSIBILITIES**

The Assistant Secretary for Administration (or designee) assures that all security policy and procedures are consistent with federal law and regulations and that adequate budget/funding for security controls and reviews is available. The Assistant Secretary (or designee) transmits documentation on the results of the DA annual security controls review to the USDA CIO.

The DA CIO will establish the process and schedule for conducting security control reviews. The DA CIO will provide oversight to the review and remediation process and ensure that deficiencies or weaknesses are communicated to the responsible Staff Office Director and that any necessary follow-up actions are being taken.

Staff Office Directors have responsibility for conducting the security controls review for the systems under their control and for implementing any corrective actions.

b **REQUIREMENTS**

An independent review by a non-DA organization, such as another USDA Agency or the Inspector General (IG), must be performed on the DA information systems annually or sooner, following any significant change, or where the risk and magnitude of harm are high.

If an external review has not been conducted, the DA CIO will schedule a review by an independent entity (government or private contractor).

Internal reviews will be performed annually at a minimum, unless an independent review has been done. They will also be performed following a significant system change, or where the risk and magnitude of harm are high. These reviews will be conducted on all DA GSSs and MAs and any systems interconnected with them. The reviews will conform to the requirements specified in the DA Information Technology Security Procedural Guidance.

Ad Hoc Reviews. Security controls must be examined as part of the investigation of any major security breach involving the GSS or MA system.

Remedial Action. The DA CIO will establish a remedial action process and periodically review its implementation. The purpose of the process is to ensure that corrective action is taken in a timely manner to correct system weaknesses found during all security control reviews (internal, USDA IG, or other external).

4 RULES OF BEHAVIOR

Rules of behavior must clearly delineate the responsibilities and expected behavior of all individuals with access to a specific system. The rules must state the consequences of inappropriate behavior. Rules of behavior are specific to each MA or GSS and must be consistent with administrative and technical security controls for these systems. Specific rules of behavior must address the use of PED's when their users are authorized to access information in the DA GSS or any of its MAs.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that: (1) rules of behavior are established and maintained for all DA GSSs and MAs; and (2) all employees and contractors have acknowledged awareness of these rules of behavior before being granted access to a GSS or MA.

Staff Office Directors have overall management responsibility for the development and implementation of the rules of behavior for the GSS and MA under their control.

b REQUIREMENTS

Rules of behavior must address responsibilities, expected behavior, and consequences for inappropriate behavior. Users must be notified of rules of behavior for any system to which they are being granted access. Users are defined as DA employees and contractor personnel.

The rules must be only as stringent as necessary to provide adequate security for the system and the information it contains. Rules must be included in the Systems Security Plans (SSPs) and made part of security awareness training. Rules must also address interconnections to other systems.

Rules of behavior for a specific system should be based on an understanding of the risk involved in the compromise or corruption of information contained in that system. If the system risk assessment is updated as a result of security controls reviews or an adverse incident, the rules of behavior should be reviewed and modified as necessary.

Users must acknowledge that they have read the rules of behavior. It is recommended that users be required to sign the rules of behavior to acknowledge that these rules have been read. Contractor personnel may be required to sign system-specific non-disclosure agreements depending on the sensitivity level of the system they are accessing.

5 LIFE CYCLE SECURITY MANAGEMENT

Security concepts and practices must be included throughout an IT system's entire life cycle in order to ensure the protection of a system and its hardware, software, firmware and data.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that security planning is addressed during the entire life cycle (including any related procurement actions) of all DA GSSs and MAs.

Staff Office Directors are responsible for overseeing the development and maintenance of full life cycle security management for all GSSs and MAs under their control.

b REQUIREMENTS

The Applications Systems Life Cycle Management Manual, DM 3200-1, from the U.S. Department of Agriculture (USDA), describes the phases of a software project as follows: Initiation (including Mission Analysis and Concept Development), Development (including System Analysis, System Design, Construction and Acquisition, testing and User Acceptance) and Operations and Maintenance. Security control requires an additional phase – Disposition – to assure proper disposal of system platforms, documents, and data at the end of its life cycle.

The phases below include, but are not limited to, the list of considerations needed to ensure the inclusion of security concepts and procedures during the life cycle. For legacy systems, only the implementation, operation and maintenance, and disposition phases may be applicable in regard to system life cycle planning.

(1) Initiation

- (a) The sensitivity of the system must be determined.
- (b) The system's business case must document the resources needed to adequately secure the system. Capital Investment requests must be fully compliant with OMB Circular A-130 direction and Information Technology Investment Portfolio System (ITIPS) procedures and include the security resources required as part of the investment portfolio.

(2) Development

- (a) An initial risk assessment must be performed in this phase to determine security requirements.
- (b) Written agreements are to be developed for the acceptance and signature of program officials. The agreements are to attest to the

acceptance of the countermeasures in the system and the residual risk inherent in the system's implementation.

- (c) Appropriate security controls must be developed for the evaluation and testing of a system before its acceptance and include the possible use of PED's. Security controls must be consistent with federal laws and regulations and USDA policies, guidelines, and standards.
- (d) All IT procurement documents must identify and include system security requirements as part of their specifications.
- (e) Procurement documents must include the ability to upgrade security controls as new threats and vulnerabilities are identified. They must also include the ability to implement new security technologies.

(3) Implementation

- (a) Security controls must be integrated into the system.
- (b) System security controls tests must be completed and documented, and the system certified prior to system implementation.
- (c) Whenever a DA IT system's security controls are modified, the security controls must be tested, and the system re-certified and re-accredited.
- (d) No DA system will be implemented prior to receiving written authorization to do so. (See Section 7 Certification and Accreditation.)

(4) Operations and Maintenance

- (a) System Security Plan (SSP) must be approved prior to initiating operation of the system. (See Section 7 Certification and Accreditation.)
- (b) The SSP must remain current during the life cycle of the system.

(5) Disposition

- (a) DA IT electronic records will be disposed of or archived in accordance with federal law and USDA policy.
- (b) Information storage media, including those in PED's, will be purged, overwritten, degaussed, or destroyed prior to disposal.

6 CONFIGURATION CHANGE MANAGEMENT

A configuration management plan must be developed and maintained throughout the system life cycle for all DA MAs and GSSs. The configuration management plan assures

that there is discipline and accountability for changes made to any system. Change management identifies the critical steps of process flow for planned and emergency change, and provides a method to evaluate success. This discipline will assure that changes do not initiate security breaches in formerly certified systems. For a GSS, the system development portions of the standard configuration management plan will not apply.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for issuing guidance on configuration management plans and ensuring that a configuration management plan is in place for each DA GSS or MA.

Staff Office Directors are responsible for establishing and maintaining a configuration management process (documented in a configuration management plan) for all MAs and GSSs under their control.

b REQUIREMENTS

No DA MA system will be modified unless the modification process is consistent with the configuration management process for that system. This applies to the full life cycle of the MA system. It includes original system development, installation, and operation functions, whether developed for DA use or obtained off-the-shelf. It also applies to any modification occurring during the operation and maintenance phase of the life cycle.

Configuration management plans must be consistent with guidelines established by USDA OCIO.

7 CERTIFICATION AND ACCREDITATION

The Certification and Accreditation (C&A) process provides assurance of the security of the system. It also establishes the level of risk that management is willing to accept in the operation of an IT system. All GSS and MA systems must be certified and accredited using the USDA OCIO Certification and Accreditation procedures.

a ROLES AND RESPONSIBILITIES

The Assistant Secretary for Administration, or designee, is the Designated Approving Authority (DAA) for all DA IT systems, in accordance with published USDA OCIO and DA policies and procedures. Acting on the advice of the Certifying Official, the DAA can accredit a system, issue an accreditation with conditions, terminate a system's operation, or not permit a system to be placed in production.

The DA CIO is the Certifying Official (CO) for all DA IT systems. The DA CIO will ensure that the USDA C&A process is employed for all DA IT systems and that the C&A process is carried out in accordance with the approved schedules

provided by each ISSPM. The DA CIO may issue a Temporary Authority to Operate (TAO) pending a full C&A determination.

b REQUIREMENTS

Each GSS and MA must be formally accredited.

In the case of a conditional accreditation, the TAO must include corrective actions, a schedule for completing them, and a statement of residual risks.

DA CIO must maintain an up-to-date inventory of systems (both developmental and operational).

8 SYSTEM SECURITY PLAN

The security requirements of a GSS or MA must be documented in a system security plan (SSP). The SSP describes the current controls and any planned controls for the system. It also delineates the security responsibilities of all persons having access to the system and defines their expected behavior when accessing the system.

a ROLES AND RESPONSIBILITIES

The DA CIO will provide guidance and ensure that System Security Plans are developed for all DA GSSs and MAs. The DA CIO must approve each SSP.

Staff Office Directors are responsible for establishing and maintaining a system security plan for all GSSs and MA systems under their control.

b REQUIREMENTS

The completion of system security plans is a requirement of Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, "Computer Security Act of 1987."

System security plans must include the procedures that implement DA IT security policies to ensure the integrity, availability, confidentiality, and continuity of the information contained in DA IT systems.

Each DA IT SSP must be updated annually or when current operating conditions or the risks to DA IT system operations change.

CHAPTER 3

OPERATIONAL CONTROLS

1 PERSONNEL SECURITY

The IT security controls set forth in this section apply to all DA personnel, including contractors, who design, implement, manage, and maintain DA IT systems. The manner in which they interact with the GSS, MA, and each other when using local and DA-wide IT systems is an important aspect of personnel security. The sensitive nature of the information in DA IT systems mandates the requirements below and USDA personnel policies be applied to DA IT systems personnel.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for:

- (1) Approving personnel security procedures related to the protection of all DA IT GSSs and MAs;
- (2) Approving requests for permission to individuals to access sensitive data in a GSS or MA prior to completion of a background check; and
- (3) Establishing a uniform DA process for requesting, establishing, and issuing IT user accounts.

Staff Office Directors are responsible for:

- (1) Establishing personnel security procedures for GSSs or MAs under their control;
- (2) Assuring that the personnel security procedures for the systems under their control are implemented and kept current;
- (3) Approving requests for permission to individuals to access non-sensitive data on a GSS or MA under their control prior to completion of a background check;
- (4) Ensuring that a uniform DA process for requesting, establishing, and issuing IT user accounts established by the DA CIO is followed; and
- (5) Ensuring the Employee Exit Procedures, DA-400-1 are followed for access to the IT user accounts.

b REQUIREMENTS

Completed background checks are mandatory for all DA and contract IT employees prior to allowing them access to DA IT systems containing sensitive information or when their role creates a significant potential for damage or

personal gain. The requirement for the appropriate level of background checks is incorporated into contract language for all DA contracts. Background checks shall be conducted in accordance with OPM 731-106, Designation of public trust positions and investigative requirements.

A sensitivity level is established for all DA IT Position Descriptions (PDs) based on the highest sensitivity level of the information processed by or contained in the GSS or MA that the incumbent of the position will access. This sensitivity level is assigned in accordance with OPM and USDA position sensitivity guidance.

Personnel security policy operates on the basis of the “Least Privilege” concept. Access to GSSs or MAs is only to the minimum degree necessary to perform a job.

Required annual reviews of personnel security procedures are conducted and all deficiencies uncovered in these reviews are corrected.

Procedures for separation of duties for personnel assigned to sensitive systems will be established and will be reflected in the PD for each position.

2 PHYSICAL AND ENVIRONMENTAL SECURITY

The information below sets the minimum standards for the physical and environmental protection of DA IT systems, buildings, and supporting infrastructure against physical and environmental threats and must include the security requirements for the use of PED’s. These requirements comply with the authorities listed in Appendix A, Authorities and References. To the extent that DA has management control of the facilities and functions addressed below, the following policies apply.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for reviewing plans for physical and environmental security and verifying that those plans are implemented.

Staff Office Directors have oversight for the physical and environmental security of any GSS or MA system under their control.

b REQUIREMENTS

All DA unit plans and operational guidelines must include the steps needed to protect IT systems from damage or destruction by manmade and non-manmade occurrences. These include, but are not limited to:

- (1) Fires or natural disasters;
- (2) Computer hacking and employee misuse;
- (3) The loss or theft of DA issued PED’s.

- (4) The maintenance of duplicate copies of data and their storage; and,
- (5) The physical protection of communications capabilities that are the responsibility of DA or are under its control.

- (a) Physical Security Controls

Buildings containing DA IT systems and/or support infrastructure must be protected by the use of guards, identification badges, and/or entry control devices such as key cards. All entry codes for cipher and electronic entry mechanisms must be changed periodically in accordance with DA physical security policies.

Access lists should be maintained for persons authorized to access DA GSS or MA sites. Only authorized persons will deposit and withdraw tapes or other storage media from libraries.

Visitors, contractors, and maintenance personnel must be authenticated and recorded prior to their entry into sensitive locations such as secured computer rooms. Physical access records must be maintained and will be audited in accordance with DA physical security policies.

Any suspicious activity by an employee or visitor must be reported to appropriate building security personnel immediately.

- (b) Fire Safety

All buildings or locations in buildings containing DA IT systems and applications must have appropriate and functioning fire prevention and suppression systems installed. These systems will be inspected and tested in accordance with building management requirements.

- (c) Utilities

Backup utility systems must be established to protect DA IT systems, applications, and data from the failure of a primary system. These are required for computer rooms, cooling systems, and electrical power.

All supporting infrastructure elements under the control of DA IT Staff Office Directors must be adequately maintained.

- (d) Data Interception or Theft

Computer monitors for personnel handling sensitive data must be located so unauthorized persons cannot view the information displayed on the monitors.

All DA sensitive information stored on mobile and portable computers and portable storage devices must be protected from unauthorized access.

3 PRODUCTION, INPUT/OUTPUT CONTROLS

DA IT support activities require that controls be established to ensure the adequate security of production, input and output support processes. This includes providing assistance to users and establishing procedures to receive, store, handle, and destroy information and its electronic or printed media.

a ROLES AND RESPONSIBILITIES

Staff Office Directors are responsible for establishing appropriate controls governing the production, input, and output of the data used by their employees and contract employees.

Federal and Contract Managers are responsible for ensuring that their employees maintain adequate control over the production, input, and output of the information for which they are responsible and/or use.

Federal and Contract Employees entering, accessing, manipulating, and extracting data housed within any DA data system must ensure that their use of DA data is in accordance with the production, input, and output controls established by the organization responsible for that data.

b REQUIREMENTS

Users must be provided with appropriate assistance to solve problems related to their use of an MA or GSS.

Access to printed, handwritten, and electronic input and output information and media must be restricted to authorized individuals. Procedures must be developed, in accordance with USDA records retention requirements, to:

- (1) Prevent the theft of electronic or printed media;
- (2) Prevent the unauthorized reading, copying, or altering of electronic or printed input or output media; and
- (3) Ensure that only authorized persons pick up, remotely access, deliver, and/or receive, electronic or printed input or output media.

Printed, handwritten, and electronic input and output information and media must be

- (1) Appropriately labeled and protected;

- (2) Stored and destroyed in accordance with current USDA record management policies; and
- (3) Must be monitored using audit trails.

4 CONTINGENCY AND DISASTER RECOVERY PLANNING

DA Staff Office system managers must develop an IT Contingency/Disaster Recovery Plan (C/DRP) for each GSS and MA under their control. Each C/DRP must provide for the timely restoration and resumption of all GSSs and MAs should they be destroyed or fail to operate.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that USDA contingency planning policy is uniformly applied across DA organizations and for coordinating DA disaster recovery planning efforts.

Staff Office Directors are responsible for ensuring the establishment of a C/DRP for each MA and GSS under their control.

b REQUIREMENTS

All Contingency/Disaster Recovery Plans prepared for DA GSSs and MAs must be based on USDA guidance.

All planning must consider requirements to support the contingency/disaster recovery plans of other USDA and federal organizations. DA IT managers must coordinate their contingency/disaster recovery planning with USDA and other federal agencies, as appropriate.

Planning must consider the type of emergency to which the plan must respond and the possible severity of the incident.

Contingency/Disaster Recovery plans must be tested annually and test results evaluated. If this evaluation indicates plan deficiencies, these deficiencies must be corrected in a timely manner as determined by the Staff Office Director in consultation with the DA CIO.

5 HARDWARE AND SOFTWARE SYSTEM MAINTENANCE

To reduce threats to the integrity, confidentiality, and availability of the information in DA IT systems, strong controls related to hardware and software installation, maintenance, and upgrading must be implemented.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that hardware and software maintenance policies, procedures, and practices for all DA GSSs and MAs are established and followed. The DA CIO approves procedures and ensures that adequate resources are planned for hardware and software maintenance performed on all DA GSSs and MAs. The DA CIO authorizes the use of shareware or copyrighted software on DA systems (GSS, MA, desktop, PED's or laptop).

Staff Office Directors are responsible for developing appropriate maintenance guidelines and procedures to protect any GSS and MA under their control, in accordance with the DA Information Technology Security Policy Instruction and the appropriate System Security Plan (SSP). Staff Office Directors authorize the use of shareware or copyrighted software on GSSs and MAs under their direct control. Staff Office Directors provide the policy for using PED's to each staff employee assigned a wireless device. The policy for PED's is presented in Appendix D.

b REQUIREMENTS

Controls addressing the installation of, and updates to, hardware and software must be established and documented. Maintenance processes must follow relevant USDA and DA procedures and must include the development of appropriate Certification and Accreditation documentation.

An inventory of hardware, including PED's, software, firmware, and their versions must be developed and maintained. Appropriate software licenses must be maintained.

Illegal or unauthorized copies of software may not be used on DA systems.

Hardware and software maintenance activities must be authorized and documented. Maintenance personnel should be allowed to access only those system elements necessary to perform their functions.

Significant maintenance changes require that security features be tested before approval is requested to return the system to operation. This requirement applies to operating systems, applications, utilities, and any other software and firmware changes to the system.

Separate procedures must be established for on-site and off-site activity. Devices should be virus checked when returned from off-site locations.

An emergency change process must be established and approved to cover situations that may require modifications to be installed within a limited time frame. This process must satisfy the SSP change management procedures for the GSSs or MAs affected within one (1) business day after the emergency installation is conducted.

6 DATA INTEGRITY

Data integrity includes the controls used to protect DA data from accidental or malicious alteration. These controls provide the user with the assurance that the data meets expectations about quality and integrity. Validation controls are comprised of the various tests and evaluations used to determine compliance with security specifications and requirements.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for oversight of the data integrity/validation controls utilized on all GSSs and MAs.

Staff Office Directors are responsible for establishing, implementing, and validating data integrity/validation controls. Staff Office Directors establish, validate, and monitor the integrity of the data on GSSs and MAs under their control. In addition, Staff Office Directors are responsible for the security of data on GSSs and MAs under their control.

b REQUIREMENTS

Data integrity controls must provide assurance to users that information has not been altered and that the system functions as expected. The data integrity process must provide for virus detection and elimination, integrity and validation controls, and penetration tests.

Virus detection systems must be updated routinely. Reconciliation testing and intrusion detection must be supported. The penetration-testing program must be a continuous program that tests each GSS and MA and its entry points. Virus patching procedures must include the testing of patches prior to request to apply the patch from the DA CIO.

7 DOCUMENTATION

The documentation of hardware, software, policies, standards, procedures, and approvals required by USDA DA provides the basis for protecting the integrity, availability, and confidentiality of IT systems.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for providing guidance and reviewing appropriate system security documentation.

Staff Office Directors are responsible for ensuring that system documentation is provided for all GSSs and MAs under their control.

b REQUIREMENTS

The availability of current documentation will aid in ensuring that all IT activities are understood and that employees have information available to carry out their duties in an efficient and effective manner. Documentation is also a key element in formalizing IT system controls.

Documentation must be available for:

- (1) System Security Plan;
- (2) Contingency/Disaster Recovery Plan;
- (3) Risk Assessment;
- (4) Rules of Behavior;
- (5) Certification and Accreditation documents and statements that authorize a system to operate;
- (6) Standard operating procedures for users, system administrators, ISSPMs, Staff Office Directors, and other managers in accordance with this document, and
- (7) Configuration/Change Management Plan

8 SECURITY AWARENESS AND TRAINING

Security awareness and training are mandatory for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of a federal agency. Security awareness and training must be provided before initial access to such systems and on a periodic refresher basis.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for:

- (1) Ensuring that an adequate IT security awareness and training program is being provided to DA employees and contractors;
- (2) Ensuring that lists of individuals who received training, and the types of training they received are maintained for two (2) years;
- (3) Ensuring that the IT security awareness and training program is developed and maintained in accordance with the USDA Computer Security Manual.

Staff Office Directors have overall management responsibility for the development of security awareness programs for the particular GSSs or MAs under their control. They also have responsibility for assuring that all of their employees and contractors have attended security awareness training sessions at the recommended times.

b REQUIREMENTS

Training is to be given as part of new employee orientation.

Refresher training is to be conducted annually.

DA staff offices must maintain records of training courses taken by employees and must maintain these records for two (2) years. This information will be provided to the DA CIO on an annual basis.

Reviews of the security and awareness training program must be conducted annually, at a minimum, and may be conducted more frequently if an incident, adverse finding or major change to a GSS or MA occurs.

Security awareness and training must encompass rules of behavior for each specific GSS and MA, and incident reporting procedures. The DA CIO will post ITSP policy, procedures, training, and awareness documents to a DA Security Page to ensure the maximum exposure of all employees to DA's ITSP.

In the event that DA issues PED's to allow remote access the GSS and its MAs, training for the users of the devices must cover the security and personal liability issues related the use of PED's. Appendix D presents the DA policy for using PED's.

All IT systems must contain a banner that warns employees that accessing the system constitutes consent to monitoring for law enforcement and other purposes. The banner must also contain a warning to unauthorized users that their use of the system may subject them to criminal prosecution and/or criminal or civil penalties.

Employee security training must be monitored and documented to ensure compliance with DA IT security training program requirements.

9 INCIDENT HANDLING, RESPONSE, AND REPORTING

The USDA Office of Operations Incident Management Handbook establishes guidance and responsibilities for the timely and effective detection, notification, reaction, investigation, response, and recovery from computer security incidents on DA IT systems and installations. USDA's Computer Incident Response Procedures Manual provides guidance on reporting incidents to the OCIO. Computer incident reporting and response procedures are designed to protect and preserve information and facilities, provide normalcy for DA users as quickly as possible, provide assistance to DA IT staff when they have an incident or suspect that an incident is occurring, and share information with other organizations, as appropriate.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for assuring there is an Incident Response procedure and that it is followed throughout DA. The DA CIO is also responsible for leading the Incident Response Team (IRT).

Staff Office Directors have responsibility for assuring that responses are handled according to DA procedures and that incidents are, reported promptly when an incident occurs within systems under their control.

b REQUIREMENTS

All DA offices will ensure that response activities meet physical and personnel security requirements at each IT system location. E-mail is particularly vulnerable to attack and should be considered separately when preparing these requirements. DA incident-related guidance must ensure:

- (1) A formal incident response capability at all locations housing an IT system or its components;
- (2) An appropriate response to alerts/advisories received from U.S. Government-operated or supported incident response organizations, e.g., Carnegie-Mellon Computer Emergency Response Team;
- (3) Monitoring of all incident responses until the problems caused by the event are corrected and documented;
- (4) Training of all persons assigned to an Incident Response Team (IRT) to ensure appropriate response to the various types of incidents and to ensure an understanding of their relationship to a Disaster Recovery Team (DRT);
- (5) The establishment of a process that allows rapid improvement of response procedures and control techniques based on the experience of previous incidents;
- (6) Efficient and effective methods that users can apply to report damaging, or potentially damaging, incidents;
- (7) An efficient and effective method for sharing vulnerability and threat information with interconnected USDA and government systems;
- (8) The sharing of incident information with the National Infrastructure Protection Center (NIPC) and, when necessary, local law enforcement; and,
- (9) The sharing of information about incidents, common vulnerabilities, and threats with the Federal Computer Incident Response Capability (FEDCIRC).

CHAPTER 4 TECHNICAL CONTROLS

1 IDENTIFICATION AND AUTHENTICATION

DA IT systems must contain technical controls that identify and authenticate users, including those using DA issued PED's, in order to prevent unauthorized access to the systems. Control measures will be in accordance with USDA policies and procedures.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that all GSS and MA systems have documented identification and authentication procedures and that these procedures are in accordance with applicable regulations and guidelines.

Staff Office Directors are responsible for managing and controlling access to all GSS and MA systems under their control and must ensure that unauthorized persons are prevented from accessing these systems. Staff Office Directors are responsible for ensuring the Employee Exit Procedures, DA-400-1 are followed for access to the systems.

b REQUIREMENTS

Access control mechanisms must support individual accountability and audit trails.

(1) Access

- (a)** Requests for specific user accounts to access any DA data or network must be approved by the Staff Office Director responsible for that user.

For audit purposes, a file of requests and decisions made on those requests must be maintained at the requesting office and the LAN/WAN administrator's office.

- (b)** Use of digital signatures will conform to federal requirements as new technology is introduced.

(2) Use

- (a)** Passwords, tokens, or other methods will be used to identify and authenticate users.
- (b)** A user's passwords, tokens, and other authentication methods related to the user will be revoked from all affected systems and applications should they be lost or compromised.
- (c)** DA IT system software must be able to correlate system activity to the user causing the activity.

- (d) Default or vendor-supplied passwords will be changed immediately upon installation of hardware, software, firmware, or an application.
- (e) If utilized, encryption methods must meet federal standards, and procedures for key management must be established.

2 LOGICAL ACCESS CONTROL

DA Staff Office system managers must establish system-based mechanisms that control the access to a specific system, including the use of PED's. The controls must define who or what is to have access to a specific system resource for the type of transactions and functions they are allowed to perform.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for ensuring that all GSSs and MAs have logical access control procedures and that these procedures are in accordance with USDA and DA regulations and guidelines.

Staff Office Directors are responsible for managing and controlling access to all GSSs and MAs under their control.

b REQUIREMENTS

(1) System Access Control Measures must:

- (a) Detect unauthorized access attempts;
- (b) Be designed to deter compromise of the integrity, availability, and confidentiality of the information in the system;
- (c) Restrict the use of security software to the Staff Office system manager or designee;
- (d) Encrypt the access control lists in accordance with federal standards;
- (e) Establish a period of user inactivity that triggers the system to do one of the following: (i) automatically blank associated display screens, (ii) disconnect the user from the system, or (iii) require the user to enter a unique password before reconnecting to the system or application;
- (f) Require internal naming conventions for access to information files that require a medium or higher degree of integrity or confidentiality; and,
- (g) Document all connections between IT systems and external systems.

(2) Telecommunications Access Controls

When access to any DA IT system via telecommunication methods is allowed, the Staff Office system manager must:

- (a) Strictly control all user remote access to IT system(s);
- (b) Maintain and review network activity logs;
- (c) Ensure that network connections automatically disconnect after a session;
- (d) Validate all connections between DA IT systems and external systems; and
- (e) Allow no guest or anonymous accounts.

(3) Firewalls and Intrusion Detection Software (IDS)

Firewalls and IDS will be used to enhance the protection of all DA IT systems. They must comply with the USDA OCIO and DA security policies and procedures.

(4) Public Access

Where the public is allowed to access a DA IT system, DA has the responsibility to take additional precautions to ensure the integrity of its systems and applications and maintain the confidence of the public. To ensure this:

- (a) The USDA privacy policy and warning itself, or a link to the page containing the privacy policy and warning, must be posted on the first page of the DA web site; and
- (b) A standardized banner must be placed over the first page of the web site that warns that the user has accessed a U.S. Government system and that unauthorized use of the system is punishable under federal law.

3 AUDIT TRAILS

Audit trails maintain records of system activity for DA GSSs and MAs. Properly collected and maintained, audit trails support reconstruction of security incidents, tracking of individual actions, and problem investigation.

a ROLES AND RESPONSIBILITIES

The DA CIO is responsible for verifying that audit trails are being kept and that audit trail logs are secured.

Staff Office Directors are responsible for ensuring that audit trails are implemented for all GSSs and MAs under their control. They are responsible for

ensuring that the audit trail administrator is not the same person who administers the access control function for the GSS or MA.

b REQUIREMENTS

Audit trails are applicable to all GSSs and MAs utilized within DA. New systems are required to include a section on audit trails in their System Security Plans. An annual review of these sections in the System Security Plan is required for existing systems with an update, if necessary.

Audit information collected must provide records of IT system activity sufficient to reconstruct any relevant security event.

APPENDIX A

Authorities and References

1. Authorities

- P. L. 90-23, The Freedom of Information Act, 1980.
- P. L. 93-579, The Privacy Act, December 1974.
- P. L. 100-235, Computer Security Act of 1987, January 1988.
- P.L. 100-503, Computer Matching and Privacy Protection Act, 1988.
- P. L. 103-62, The Government Performance and Results Act of 1993.
- P. L. 104-13, Paperwork Reduction Act of 1995.
- P. L. 104-106, Clinger-Cohen Act of 1996.
- P. L. 107-347 Title III, Federal Information Security Act of 2002.
- E. O. 13010, Critical Infrastructure Protection, October 2001.
- E. O. 13011, Federal Information Technology.
- E. O. 13013, Computer Software Privacy.
- Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.
- Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.
- Office of Management and Budget (OMB) Memorandum M-02-1, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 17, 2001.
- Office of Management and Budget (OMB) Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, January 16, 2001.
- Office of Management and Budget (OMB) Memorandum M-01-24, Reporting Instructions for the Government Information Security Act, June 22, 2001.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, November 30, 2000 and Appendix III, Security of Federal Automated information Resources.
- Office of Management and Budget (OMB) Bulletin 90-08, "Guidance for Preparation of Security Plans for Computer Systems that Contain Sensitive Information," July 9, 1990.
- Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Automated Information Systems," February 1996.
- 29 CFR Part 70, USDA Regulations Implementing the Privacy Act.
- Department of Agriculture, Departmental Regulation 3140-001, "USDA Information Systems Security Policy".

Department of Agriculture, Departmental Regulation 3140-002, “USDA Internet Security Policy”.

Department of Agriculture, Departmental Regulation, “Telecommunications and Internet Services and Use.

Department of Agriculture, Cyber Security Office, “Information Systems Security Assessment Guide. Version 1.0, April 12, 2001.

APPENDIX A

Authorities and References (Continued)

2. References

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

Federal Information Processing Standards Publication (FIPS PUB) 87, “Guidelines for Automated Data Processing Contingency Planning,” March 27, 1981.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

General Accounting Office, Executive Guide, Information Security Management, May 1998.

Hamilton, Caroline Ramsey, Data-Driven Security, How to Target, Focus and Prioritize the Security Program, ISSA Password, July-August, 2001.

National Communications System, Public Switched Network Security Assessment Guidelines, September 2000.

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, January 2002.

NIST Special Publication 800-26, Security Self Assessment Guide for Information Technology Systems, January 2002.

NIST Special Publication 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

National Institute of Standards and Technology's (NIST) draft Special Publication, Self-Assessment Guide for Information Technology Systems, March 9, 2001.

National Institute of Standards and Technology (NIST), NISTIR 5153, “Minimum Security Requirements for Multi-user Operating Systems,” March 1993.

Computer Emergency Response Team (CERT) Coordination Center, Carnegie Mellon University, “LIWA Incident Handling for Managers,” May 1998.

Draft Federal Sector Critical Infrastructure Protection Plan, prepared by the Critical Infrastructure Protection Task Force, dated October 7, 1998.

National Institute of Standards and Technology (NIST), Special Publication 800-3, “Establishing a Computer Security Incident Response Capability (CSIRC),” November 1991.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, “Guide for Developing Security Plans for Information Technology Systems,” December 1998.

U. S. Department of Justice, “Information Technology Security,” July 12, 2001.

APPENDIX B

Terms and Definitions

Access	The opportunity to make use of an information system (IS) resource.
Access Control	The limiting of access to information system resources to authorized users, program, processes, and controls.
Accountability	The principle that responsibilities for ownership and/or oversight of IS resources are explicitly assigned and that assignees are answerable to proper authorities for the stewardship of resources under their control.
Agency	A federal department, major organizational unit in a department, or independent agency
Application	A software package designed to perform a specific set of functions, such as word processing, or communications. See also program .
Attack	An intentional attempt to bypass the physical or information security measures and controls protecting an IS.
Audit	An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established security policies and procedures, and/or to recommend necessary changes in controls, policies, or procedures to meet security objectives.
Audit Trail	A chronological record of system activities or message routing that permits reconstruction and examination of a sequence of events.
Authentication	A security measure designed to measure the validity of a transmission, message, or originator; or as a means of verifying a user's authorization to access specific types of information.
Banner	A display on an IS that sets forth conditions and restrictions on a system and/or data use.
Confidentiality	An assurance that information is not disclosed to unauthorized persons, processes, or devices.

APPENDIX B
Terms and Definitions (Continued)

Configuration Management	The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IS.
Contingency Plan	A plan maintained for emergency response, backup operations, and post-disaster recovery of an IS, to ensure availability of critical resources and facilitate the continuity of operations in an emergency.
Cryptography	The science of encrypting (coding) plain data and information into a form intelligible only to authorized persons who are able to decrypt (decode) it.
Data Integrity	A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Disaster Recovery	A plan describing the process of restoring an IS to full operation after an interruption in service, including equipment repair/replacement, file recovery/restoration and the resumption of service to users. (Also known as Business Resumption)
Disaster Recovery Plan	The plan used to guide an organization's disaster recovery effort.
Disaster Recovery Team	The group of persons, selected for their specific skills, that are used to execute a Disaster Recovery Plan
E-mail	The abbreviation for electronic mail, which consists of messages sent over an IS by communications applications. E-mail that is sent from one computer system or another or over the Internet must pass through gateways to leave the originating system and to enter the receiving system.
Environment	The total of the external procedures, conditions, and objects affecting the development, operation, and maintenance of an IS.
Federal Computer Incident Response Capability	The U.S. Government's focal point for handling computer security related incidents.

APPENDIX B
Terms and Definitions (Continued)

Firmware	An application recorded in permanent or semi-permanent computer memory.
Gateway	An interface between networks that facilitates compatibility by adapting transmission speeds, protocols, codes, or security measures.
General Support System	An interconnected set of information resources under the same direct management control which shares common functionality. A general support system normally includes hardware, software, information, data, non-major applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization.
Incident	An occurrence that has been assessed as having an adverse effect on the security or performance of an IS.
Incident Response Team	The group of persons, selected for their specific skills that are used to correct the effects of an IT incident.
Information Systems	All the electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. An IS may be automated (e.g., a computerized IS) or manual (e.g., papers in a file).
Information Systems Security	The measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. This is also called computer security.
Information System Security Program Manager	The person assigned to implement an organization's information system security policy.

APPENDIX B

Terms and Definitions (Continued)

Integrity	The condition existing when an IS operates without unauthorized modification, alteration, impairment, or destruction of any of its components.
Interface	A common boundary or connector between two applications or devices, such as a graphical user interface (GUI) that allows a user to interact with an application written in code.
Intrusion	Attacks or attempted attacks from outside the security perimeter of an IS.
Laptop Computer	A portable computer usually powered by a rechargeable battery. The smaller versions are also called notebook computers.
Major Application	<p>An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.</p> <p>Local programs designed to meet particular office and standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or other general- purpose software) are generally not considered major applications and would usually be covered by the security policies and procedures for the general support system on which they are installed. Certain of these applications, however, because of the sensitive information in them, require special management oversight and should be treated as major.</p>
National Infrastructure Protection Center	The U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks on its critical infrastructures.
Network Security	The security procedures and controls that protect a network from: (1) unauthorized access, modification, and information disclosure; and (2) physical impairment or destruction.

APPENDIX B

Terms and Definitions (Continued)

Non-repudiation	A cryptographic service that legally prevents the originator of a message from denying authorship at a later date.
Operating system	The software required by every computer that: (1) enables it to perform its basic tasks such as controlling disks, drives, and peripheral devices; and (2) provides a platform on which applications can operate.
Operational Controls	The security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Password	A string of characters containing letters, numbers, or other keyboard symbols that is used to authenticate a user's identity or authorize access to data. Only the authorized user who originated it generally knows the password.
Policy	A document that delineates the security management structure, clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.
Personal Electronic Devices (PED)	A hand held or larger device that may upload, download, or remotely access information in the DA GSS and/or its MAs. These include, but are not limited to, laptop and notebook computers, cellular phones that may transmit data or e-mail, Personal Data Assistants (PDA), wireless access devices, portable storage drives, etc.
Procedures	A document that focuses on the security control areas and management's position.
Program	A set of instructions in code that, when executed, cause a computer to perform a task.
Risk	The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

APPENDIX B

Terms and Definitions (Continued)

Risk Management	The ongoing process of assessing the risk to automated information resources and information. Part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.
Rules of Behavior	The rules that are established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, assignment and limitation of system privileges, and individual accountability.
Sensitive Information	Unclassified information, the loss, misuse, or unauthorized disclosure of which could adversely affect the national security interest, the conduct of federal programs, or the privacy of individuals protected by the Privacy Act (5 U.S.C. Section 552a). Information systems containing sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). (This information is also called Sensitive but Unclassified (SBU)).
Software	The electronically stored commands and instructions that make an IS functional, including the operating system, applications, and communications protocols.
Staff Office System Manager	The person responsible for the life cycle operation of an IT system, including the implementation of standard procedures and controls to enforce an organization's security policy.
System Integrity	Optimal functioning of an IS, free from unauthorized impairment or manipulation.

APPENDIX B
Terms and Definitions (Continued)

System Security Plan

A formal document listing the tasks necessary to meet system security requirements, a schedule for their accomplishment, and where the responsibilities for each task are assigned.

Vulnerability

A flaw in security procedures, software, internal system controls or implementation of an IS that may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.

APPENDIX C

Acronyms and Abbreviations

C&A	Certification and Accreditation
C/DRP	Contingency/Disaster Recovery Plan
CIO	Chief Information Officer
CO	Certifying Official
COTR	Contracting Officer's Technical Representative
DA	Departmental Administration
DAA	Designated Approving Authority
DRT	Disaster Recovery Team
FEDCIRC	Federal Computer Incident Response Capability
GAO	Government Accounting Office
GSS	General Support System
IG	Inspector General
IRM	Information Resources Management
IRT	Incident Response Team
IS	Information System
ISSPM	Information System Security Program Manager
IT	Information Technology
ITIPS	Information Technology Investment Portfolio System
ITS	Information Technology Security
ITSP	Information Technology Security Program
LAN	Local Area Network
MA	Major Application
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OO	Office of Operations
P. L.	Public Law
PD	Position Description
PED	Personal Electronic Device
RFP	Requests for Proposal

APPENDIX C
Acronyms and Abbreviations (Continued)

SBU	Sensitive but Unclassified
SSAA	System Security Authorization Agreement
SSP	System Security Plan
TAO	Temporary Authority to Operate
USDA	Department of Agriculture
WAN	Wide Area Network

APPENDIX D
DA Policy On Use of
Personal Electronic Devices

1. Personal Electronic Devices (PED's) will not be used for official business unless the CIO grants an approved waiver of this policy and procedures.
2. Changes will not be made in official system configurations, operating or antivirus software or remote access arrangements as required by the person using the PED, except by the agency IT staff.
3. Modems will remain disabled.
4. In absence of electronic verification or auditing, physical inventories of PED's will be done on an annual basis.
5. During the annual inventory, storage of information will be checked to confirm only required information is maintained and that Sensitive but Unclassified (SBU) data is encrypted.
6. During travel, PED's will be handcarried to prevent damage or theft.
7. The agency contact person will be contacted immediately in case of loss or theft of the PED.
8. PED's will be returned to the agency on a regular basis for system updates, patches and accountability reasons.
9. Encryption techniques will be used for infrared and wireless transmissions of SBU information or for storage of SBU data.
10. PED's will be surrendered to the agency or staff office immediately upon transfer, reassignment, resignation or retirement from federal service.
11. Unauthorized software and unauthorized copyrighted or illegal material will not be loaded or stored on PED.
12. Care will be exercised in discussions of sensitive information using wireless technology to prevent inadvertent disclosure of SBU or violations of the Privacy Act.
13. Floppy disks, CD-Rom, and Flash Memory will not be used to download applications or SBU information in violations of security policy.